

Title (en)
UPDATABLE PRIVATE SET INTERSECTION

Title (de)
AKTUALISIERBARE PRIVATE SATZKREUZUNG

Title (fr)
INTERSECTION ACTUALISABLE D'ENSEMBLES PRIVÉS

Publication
EP 4226568 A4 20240612 (EN)

Application
EP 21878153 A 20210519

Priority
• US 202063089359 P 20201008
• US 2021033163 W 20210519

Abstract (en)
[origin: WO2022076038A1] "Updatable" private set intersection (PSI) protocols allow parties that each have an updatable private set to determine the intersection of their sets after an update without the need to compare each element of each set and without compromising privacy. In some protocols, a first party can determine an update to the intersection by determining an intersection of elements that were previously in the first party's set with elements that were added to the second party's set and determining an intersection of elements that were added to the first party's set with elements that are in the second party's (updated) set. In some protocols, both parties can determine the updated intersection.

IPC 8 full level
H04L 9/08 (2006.01); **G06F 21/60** (2013.01); **G06F 21/62** (2013.01); **H04L 9/00** (2022.01); **H04L 9/06** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)
G06F 16/2246 (2019.01 - US); **G06F 16/24558** (2019.01 - US); **G06F 21/602** (2013.01 - US); **G06F 21/6245** (2013.01 - EP);
H04L 9/008 (2013.01 - EP); **H04L 9/0841** (2013.01 - EP); **H04L 9/3239** (2013.01 - EP); **H04L 2209/50** (2013.01 - EP)

Citation (search report)
• [A] US 2020195618 A1 20200618 - LINTON JEB R [US], et al
• [A] KACSMAR BAILEY ET AL: "Differentially Private Two-Party Set Operations", 2020 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY (EUROS&P), IEEE, 7 September 2020 (2020-09-07), pages 390 - 404, XP033847065, DOI: 10.1109/EUROSP48549.2020.00032
• [A] HAO CHEN ET AL: "Labeled PSI from Fully Homomorphic Encryption with Malicious Security", COMPUTER AND COMMUNICATIONS SECURITY, ACM, 2 PENN PLAZA, SUITE 701NEW YORKNY10121-0701USA, 15 January 2018 (2018-01-15), pages 1223 - 1237, XP058418218, ISBN: 978-1-4503-5693-0, DOI: 10.1145/3243734.3243836
• See also references of WO 2022076038A1

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)
WO 2022076038 A1 20220414; CN 116324778 A 20230623; EP 4226568 A1 20230816; EP 4226568 A4 20240612;
US 2023359631 A1 20231109

DOCDB simple family (application)
US 2021033163 W 20210519; CN 202180067200 A 20210519; EP 21878153 A 20210519; US 202118028696 A 20210519